



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/767,868	01/28/2004	Marco Casassa Mont	B-5362 621671-4	4129

22879 7590 10/09/2007
HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER

GYORFI, THOMAS A

ART UNIT	PAPER NUMBER
----------	--------------

2135

MAIL DATE	DELIVERY MODE
-----------	---------------

10/09/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/767,868	Applicant(s) MONT ET AL.	
	Examiner Tom Gyorfi	Art Unit 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-60 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-60 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|--|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>1/28/04 and 9/7/04</u> . | 6) <input type="checkbox"/> Other: ____ |

DETAILED ACTION

1. Claims 1-60 are pending examination.

Information Disclosure Statement

2. The information disclosure statements (IDS) submitted on 1/28/04 and 9/7/04 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statements are being considered by the examiner.

Priority

3. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-26, 30, 34-50, and 52-60 are rejected under 35 U.S.C. 102(b) as being anticipated by Sweet et al. (U.S. Patent Application Publication 2002/0031230).

Art Unit: 2135

Regarding claims 1 and 53:

Sweet discloses a privacy management method comprising: first operation, effected by an owner of personal data, comprising: encrypting that data based on encryption key string formed using at least policy data indicative of conditions, differing from recipient identity, to be satisfied before access is given to said personal data, and public data provided by a trusted party and related to private data of the latter (paragraphs 0012 and 0128-0131); providing the encrypted data to a recipient (paragraph 0145); second operations, effected by a trusted party, comprising using the encryption key string and said private data to determine a decryption key, and outputting this key (paragraph 0147); at least one of these second operations only being effected after a further second operation has checked that said conditions are satisfied regarding said recipient (paragraph 0145).

Regarding claim 37:

Sweet discloses a privacy management system comprising first, second, and third computing entities, wherein: the first computing entity comprises: a data store for holding personal data (paragraph 0026); an encryption unit for encrypting the personal data based on encryption parameters comprising both an encryption key string formed using at least policy data indicative of conditions, differing from recipient identity, to be satisfied before access is given to said personal data, and public data provided by a trusted party and related to private data of the latter (paragraphs 0012 and 0128-0131); and a communications interface for providing the encrypted data to the third computing

Art Unit: 2135

entity (paragraph 0145); the second computing entity comprises a data store for holding said private data (paragraph 0026); a communications interface for receiving the encryption key string and for providing a corresponding decryption key to the third computing entity (paragraphs 0129-0131); a decryption key determination unit for using the private data and the received encryption key string to determine the corresponding decryption key for decrypting the encrypted data (paragraph 0132-0133); and a condition-checking arrangement for ensuring that the decryption key is only determined, or only provided to the third computing entity, after the conditions in said policy data have been satisfied in respect of the third computing party (paragraph 0145).

Regarding claim 53:

Sweet discloses a computing entity arranged to act as a trusted party, the computing entity comprising: a data store for holding said private data (paragraph 0026); a communications interface for receiving the encryption key string and for providing a corresponding decryption key to the third computing entity (paragraphs 0129-0131); a decryption key determination unit for using the private data and the received encryption key string to determine the corresponding decryption key for decrypting the encrypted data (paragraph 0132-0133); and a condition-checking arrangement for ensuring that the decryption key is only determined, or only provided to the third computing entity, after the conditions in said policy data have been satisfied in respect of the third computing party (paragraph 0145).

Art Unit: 2135

Regarding claims 2 and 38:

Sweet further discloses wherein the first operations further comprise providing the encryption key string to said recipient along with the encrypted data (paragraph 0129); the method further comprising intermediate operations in which the recipient receives the trusted third party with the encryption key string and requests the decryption key (Ibid).

Regarding claim 3:

Sweet further discloses wherein the first operations further comprise providing details of the trusted party to said recipient along with the encrypted data (para. 0134).

Regarding claims 4 and 39:

Sweet further discloses further said recipient sending on the encrypted personal data to a further party, and the trusted party providing the decryption key to that further party only after said conditions have been satisfied in respect of that further party (paragraphs 0139-0142).

Regarding claim 5:

Sweet further discloses wherein in said first operations multiple items of personal data are encrypted each using said public data and a respective encryption key string formed using at least respective policy data, the encrypted multiple items being provided to said recipient, and wherein the second operations the trusted party

Art Unit: 2135

determines the decryption key for at least one encrypted item using the corresponding encryption key string and said private data, the or each determined decryption key only being provided to said recipient after the conditions in the corresponding policy have been satisfied (paragraph 0129, and elements 220a-d of Figure 2).

Regarding claim 6:

Sweet further discloses said recipient sending on a selected subset of said multiple encrypted items of personal data to a further party; and the trusted party providing to that further party a decryption key for an encrypted item provided to that party, only after the conditions in the corresponding policy data have been satisfied in respect of said party (paragraphs 0135-0140).

Regarding claim 7:

Sweet further discloses wherein the data owner has a set of policies that form respective nodes in a policy hierarchy, and wherein in said first operations, multiple items of personal data are encrypted and provided to said recipient, each such data item being independently associated with at least one node of the policy hierarchy and being encrypted using said public data and policy data formed by a concatenation of the policies of the nodes traversed between the root of the hierarchy and the said at least one node with which the data item is associated (paragraphs 0032 and 0140).

Art Unit: 2135

Regarding claim 8:

Sweet further discloses wherein the data owner has a set of policies that form respective nodes in a policy hierarchy, and wherein in said first operations, multiple items of personal data are encrypted and provided to said recipient, each such data item being independently associated with at least one node of the policy hierarchy and being encrypted by an iterative process in which: the data item is encrypted using said public data and policy data formed by the policy of the said at least one associated node, the encrypted data thus produced then becoming a data item associated with the parent node of the or each node formed by the policy just used for encryption (Ibid).

Regarding claim 9:

Sweet further discloses wherein in said first operations, multiple items of personal data are encrypted and provided to said recipient, at least two of these data items being encrypted using public data of different respective trusted parties whereby the recipient must obtain the appropriate decryption key from a different one of the trusted parties in dependence on which data item the recipient wishes to access (paragraphs 0138-0140).

Regarding claim 10:

Sweet further discloses wherein in said first operations an item of personal data is first encrypted using a first policy and the public data of a first trusted party with the encrypted data being then further encrypted using a second policy and the public

Art Unit: 2135

data of a second trusted party whereby the recipient must obtain decryption keys from the two trusted parties in order to access the data item (paragraphs 0019 and 0115).

Regarding claim 11:

Sweet further discloses wherein in said first operations the personal data is encrypted using public data provided by multiple trusted parties, the second operations being carried out by each of said multiple trusted parties to provide a respective decryption sub-key whereby to enable the recipient to decrypt the encrypted personal data by the combined use of the sub-keys from each trust authority; each trusted party ensuring that policy conditions for which it is competent have been satisfied before generating and/or outputting the corresponding sub-key (paragraphs 0135-0147).

Regarding claims 12, 40, and 54:

Sweet further discloses wherein the trusted party makes an audit record of each provision of a decryption key by the trusted party (paragraphs 0300-0304).

Regarding claims 13, 41, and 55:

Sweet further discloses wherein said audit record further comprises information about when a decryption key is not provided because a related policy condition has not been satisfied, this information including information about the condition failure (paragraphs 0284-0295).

Art Unit: 2135

Regarding claims 14, 42, and 56:

Sweet further discloses wherein the trusted party on receiving a request from a party for a decryption key in respect of a particular item of data, checks its audit records to ascertain whether the decryption key for that item has previously been provided to a different party, and if so, whether the policy associated with the data item permitted onward disclosure (Ibid, and paragraph 0225).

Regarding claims 15 and 57:

Sweet further discloses wherein the trusted party, on determining that the decryption key for the data item was previously provided under a policy of no onward disclosure, refuses to provide the decryption key to the requesting party (Ibid).

Regarding claim 16:

Sweet further discloses wherein the first and second operations are repeated multiple times for the same or different personal data owned by the same or different personal-data owners and provided to the same or different recipients (paragraphs. 0139 and 0225).

Regarding claims 17 and 44:

Sweet further discloses wherein the trusted party makes an audit record of each provision of a decryption key by the trusted party (paragraphs 0297-0302).

Art Unit: 2135

Regarding claims 18 and 45:

Sweet further discloses wherein said audit record comprises the identity of the personal data, personal-data owner and recipient concerned (Ibid).

Regarding claims 19 and 46:

Sweet further discloses wherein said audit record further comprises information about when a decryption key is not provided because a related policy condition has not been satisfied, this information including information about the condition failure (paragraphs 0290-295).

Regarding claims 20 and 47:

Sweet further discloses wherein the trusted party on receiving a request from a party for a decryption key in respect of a particular item of data, checks its audit records to ascertain whether the decryption key for that item has previously been provided to a different party, and if so, whether the policy associated with the data item permitted onward disclosure (paragraphs 0137-0142).

Regarding claim 21:

Sweet further discloses wherein the trusted party, on determining that the decryption key for the data item was previously provided under a policy of no onward disclosure, refuses to provide the decryption key to the requesting party (para. 0225).

Art Unit: 2135

Regarding claim 22:

Sweet further discloses wherein a said policy condition relates to the strength of cryptographic methods to be employed in authenticating the identity of the recipient before the decryption key is provided to the latter (paragraph 0142).

Regarding claim 23:

Sweet further discloses wherein a said policy condition relates to the expiry date of the policy or of the personal data, the trusted party not providing the decryption key when the expiry date has passed (paragraph 0040).

Regarding claims 24, 48, and 58:

Sweet further discloses wherein a said policy condition relates to the trusted party communicating with the owner, the trusted party effecting this communication before providing the decryption key to said recipient (paragraph 0040).

Regarding claims 25, 49, and 59:

Sweet further discloses wherein the condition is that the trusted party obtain consent from the owner before providing the decryption key to said recipient (Ibid).

Regarding claims 26 and 50:

Sweet further discloses wherein contact details for the owner are contained in policy data in encrypted form, the contact details being encrypted using said public

Art Unit: 2135

data of the trusted party and an encryption key string formed by a data element also included in the policy data whereby the trusted party can form the corresponding decryption key and decrypt the encrypted contact details (paragraph 0134).

Regarding claim 30:

Sweet further discloses wherein the software being run by the computing entity of the recipient is arranged to prevent onward disclosure of data indicated in a predetermined manner, the data owner marking an item of personal data in this predetermined way before providing it to the recipient (paragraphs 0138-0142).

Regarding claims 34 and 52:

Sweet further discloses wherein the owner of the personal data also serves as the trusted party (paragraphs 0019 and 0028).

Regarding claim 35:

Sweet further discloses wherein said owner is acting as a proxy for a party to whom the personal data relates (paragraph 0213).

Regarding claim 36:

Sweet further discloses wherein in the second operations the decryption key is not determined until after said conditions have been satisfied (paragraph 0145).

Art Unit: 2135

Regarding claim 43:

Sweet further discloses multiple first and third computing entities, the second computing entity being arranged to provide decryption keys for the third computing entities in respect of personal data encrypted by the first computing entities provided the corresponding policy conditions have been satisfied in each case (paragraph 0129).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 27-29, 31-33 and 51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sweet as applied to claims 1 and 37 above, and further in view of "Trusted Computing Platforms: TCPA Technology in Context" (hereinafter, "Balacheff").

Regarding claims 27-29, 31-33, and 51:

Sweet does not explicitly disclose requiring the use of a trusted platform running software of predetermined functionality that cannot be subverted. However, the use of trusted computing platforms using dedicated hardware to ensure that said platform is running software of predetermined functionality that cannot be subverted was known in the art (Balacheff, Chapter 2, "Scenario 2: Checking Client Integrity"). Note also that TPMs are also useful in identity attestation, as per the Sweet disclosure (Balacheff,

Art Unit: 2135

Chapter 2, "Scenario 4: Remote Attestation"). All of the claimed elements were known in the prior art, and one skilled in the art could have combined the elements as claimed by known methods with no change in their respective functions, and the combination would have yielded predictable results to one of ordinary skill in the art at the time of the invention.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. U.S. Patent 6,349,338 to Seamons et al., and U.S. Patent Application Publication 2002/005556 to Shah et al.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tom Gyorfí whose telephone number is (571) 272-3849. The examiner can normally be reached on 8:30am - 5:00pm Monday - Friday.

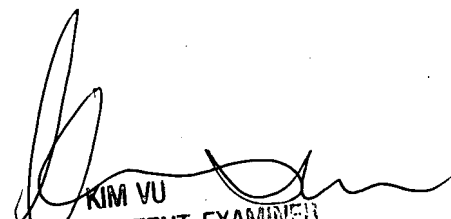
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

Art Unit: 2135

For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TAG
9/28/07


KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100